Great Theoretical Ideas In Computer Science

Victor Adamchik — CS 15-251 — Spring 2010

Danny Sleator

Lecture 17 — Mar. 17, 2010 — Carnegie Mellon University

Algebraic Structures: Group Theory II

Group

A group G is a pair (S,♦), where S is a set and ♦ is a binary operation on S such that:

1. **♦ is associative**

2. **(Identity) There exists an element e ∈ S such that:**
   e ♦ a = a ♦ e = a, for all a ∈ S

3. **(Inverses) For every a ∈ S there is b ∈ S such that:**
   a ♦ b = b ♦ a = e

Review

order of a group G = size of the group G

order of an element g = (smallest n>0 s.t. g^n = e)

g is a generator if order(g) = order(G)

Orders

Theorem:

Let x be an element of G. The order of x divides the order of G

Orders: example

$(Z_{10}: +)$

{0,1,2,3,4,5,6,7,8,9}

smallest n>0 such that $g^n = e$

1 10 5 10 5 2

Subgroups

Let G be a group. A non-empty set H G is a subgroup if it forms a group under the same operation.

Exercise.

Does {0,2,4} form a subgroup of Z_6 under +?

Exercise.

Does $\{2^n, n \in Z\}$ form a subgroup of $Q\setminus\{0\}$ under *?

Subgroups

Let G be a group. A non-empty set H G is a subgroup if it forms a group under the same operation.

Exercise.
List all subgroups of Z_{12} under +.

Z_{12} {0} {0,6} {0,4,8} {0,3,6,9}

{0,2,4,6,8,10}

Cosets

We are going to generalize the idea of congruent classes mod n in (Z,+).

$a = b \pmod n$ iff $a - b \in \langle n \rangle$

Theorem. Let H is a subgroup of G.
Define a relation: $a \sim b$ iff $a \diamond b^{-1} \in H$.
Then $\sim$ is an equivalence relation.

Cosets

Theorem. Let H is a subgroup of G.
Define a relation: $a \sim b$ iff $a \diamond b^{-1} \in H$.
Then $\sim$ is an equivalence relation.

Proof. Reflexive: $a \sim a$ iff $a \diamond a^{-1} = e \in H$

Symmetric: $b \diamond a^{-1} = (a \diamond b^{-1})^{-1} \in H$

Transitive: $a \diamond c^{-1} = (a \diamond b^{-1})(b \diamond c^{-1}) \in H$

Cosets

The equivalent classes for this relation is called the right cosets of H in G.

If H is a subgroup of a group G then for any element g of the group the set of products of the form $h \diamond g$ where $h \in H$ is a right coset of H denoted by the symbol Hg.

Cosets

Exercise.
Write down the right coset of the subgroup {0,3,6,9} of Z_{12} under +.

Right coset = $\{h\ g \mid h \in H, g \in G\}$

{0,3,6,9} + {0,1,2,3,4,5,6,7,8,9,10,11} =

[3]+0 = {0,3,6,9}
[3]+1 = {1,4,7,10}
[3]+2 = {2,5,8,11}

Cosets

Theorem.
If H is a finite subgroup of G and $x \in G$, then $|H| = |Hx|$

Proof. We prove this by finding a bijection between H and Hx.

It is onto, because Hx consists of the elements of the form hx, where $h \in H$.

Assume that there are $h_1, h_2 \in H$. .

Then $h_1 x = h_2 x$. It follows, $h_1 = h_2$.

Cosets: partitioning

Theorem.
If H is a finite subgroup of G, then $G = \cup_{x \in G} Hx$.

Proof. Cosets are equivalent classes.
The two cosets are either equal or disjoint.

Since G is finite, there are finitely many such cosets.

Every element x of G belongs to the coset determined by it.

$x = x\,e \in Hx$, since $e \in H$.

Lagrange's Theorem

Theorem:
If G is a finite group, and H is a subgroup then the order of H divides the order of G.

In symbols, |H| divides |G|.

Lagrange's Theorem

Theorem: |H| divides |G|.

Proof: G is partitioning into cosets.
Pick a representative from each coset
$G = \cup_{j=1\ldots k} Hx_j$

Each coset contains |H| elements.

It follows |G| = k |H|. Thus |H| is a divisor of |G|.

Lagrange's Theorem: what is for?

The theorem simplifies the problem of finding all subgroups of a finite group.

Consider group of symmetry of square

$Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_|, F_-, F_/, F_\backslash \}$

Except $\{R_0\}$ and Y_{sq}, all other subgroups must have order 2 or 4.

Order 2

	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_\backslash$	$F_/$	$F_|$	F_-
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_-	$F_|$	$F_\backslash$	$F_/$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_/$	$F_\backslash$	F_-	$F_|$
$F_|$	$F_|$	$F_/$	F_-	$F_\backslash$	R_0	R_{180}	R_{90}	R_{270}
F_-	F_-	$F_\backslash$	$F_|$	$F_/$	R_{180}	R_0	R_{270}	R_{90}
$F_/$	$F_/$	F_-	$F_\backslash$	$F_|$	R_{270}	R_{90}	R_0	R_{180}
$F_\backslash$	$F_\backslash$	$F_|$	$F_/$	F_-	R_{90}	R_{270}	R_{180}	R_0

Order 4

	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_\backslash$	$F_/$	$F_|$	F_-
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_-	$F_|$	$F_\backslash$	$F_/$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_/$	$F_\backslash$	F_-	$F_|$
$F_|$	$F_|$	$F_/$	F_-	$F_\backslash$	R_0	R_{180}	R_{90}	R_{270}
F_-	F_-	$F_\backslash$	$F_|$	$F_/$	R_{180}	R_0	R_{270}	R_{90}
$F_/$	$F_/$	F_-	$F_\backslash$	$F_|$	R_{270}	R_{90}	R_0	R_{180}
$F_\backslash$	$F_\backslash$	$F_|$	$F_/$	F_-	R_{90}	R_{270}	R_{180}	R_0

Lagrange's Theorem

Exercise.

Suppose that H and K are subgroups of G and assume that

$$|H| = 9,\ |K| = 6,\ |G| < 50.$$

What are the possible values of $|G|$?

LCM(9,6) = 18, so $|G|$=18 or 36

Isomorphism

Mapping between objects, which shows that they are structurally identical.

Any property which is preserved by an isomorphism and which is true for one of the objects, is also true of the other.

Isomorphism

Example.

{1,2,3,…}, or {I, II, III,…}, or {один, два, три,…}

Mathematically we want to think about these sets as being the same.

Group Isomorphism

Definition. Let G be a group with operation $*$ and H with $\blacklozenge$.

An isomorphism of G to H is a bijection $f: G \longrightarrow H$ that satisfies

$$f(x * y) = f(x) \blacklozenge f(y)$$

If we replace bijection by injection, such mapping is called a homomorphism.

Group Isomorphism

Example.

$$G = (Z, +),\ H = (\text{even}, +)$$

Isomorphism is provided by $f(n) = 2n$

$f(n + m) = 2(n+m) = (2n)+(2m)=f(n)+f(m)$

Group Isomorphism

Example.

$$G = (R^+, *),\ H = (R, +)$$

Isomorphism is provided by $f(x) = \log(x)$

$f(x * y) =$

$\log(x * y) = \log(x) + \log(y) = f(x) + f(y)$

Group Isomorphism

Theorem. Let G be a group with operation $*$, H with $\blacklozenge$ and they are isomorphic $f(x * y) = f(x) \blacklozenge f(y)$. Then $f(e_G) = e_H$

Proof. $f(e_G) = f(e_G * e_G) = f(e_G) \blacklozenge f(e_G)$.

On the other hand, $f(e_G) = f(e_G) \blacklozenge e_H$

$f(e_G) \blacklozenge e_H = f(e_G) \blacklozenge f(e_G) \Longrightarrow f(e_G) = e_H$

Group Isomorphism

Theorem. Let G be a group with operation $*$, H with $\blacklozenge$ and they are isomorphic $f(x * y) = f(x) \blacklozenge f(y)$. Then $f(x^{-1}) = f(x)^{-1}$, $x \in G$

Proof.

$f(x) \blacklozenge f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_H$.

Group Isomorphism

In order to prove that two groups and are not isomorphic, one needs to demonstrate that there is no isomorphism from onto .

Usually, in practice, this is accomplished by finding some property that holds in one group, but not in the other.

Examples. $(Z_4, +)$ and $(Z_6, +)$
They have different orders.

Group Isomorphism

Exercise.
Verify that $(Z_4, +)$ is isomorphic to $(Z^*_5, *)$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Exercise.
Verify that $(Z_4, +)$ is isomorphic to $(Z^*_5, *)$

Z_4 is generated by 1 as in 0, 1, 2, 3, (then back to 0)

Z^*_5 is generate by 2 as in 1, 2, 4, 3, (then back to 1)

$0 \leftrightarrow 1$
$1 \leftrightarrow 2$
$2 \leftrightarrow 4$
$3 \leftrightarrow 3$

$f(x) = 2^x \bmod 5$

Cyclic Groups

Definition. Let G be a group and $x \in G$. Then $\langle x \rangle = \{x^k \mid k \in Z\}$ is a cyclic subgroup generated by x.

Examples.
$(Z_n, +) = \langle 1 \rangle$
$(Z^*_5, *) = \langle 2 \rangle$ or $\langle 3 \rangle$

Cyclic Groups

Theorem. A group of prime order is cyclic, and furthermore any non-identity element is a generator.

Proof. Let $|G|=p$ (prime) and $x \in G$.

By Lagrange's theorem, order(x) divides $|G|$.

Since p is prime, there are two divisors 1 and p. Clearly it is not 1, because otherwise x=e.

Cyclic Groups

Theorem. Any finite cyclic group of order n is isomorphic to $(Z_n,+)$.

Any infinite cyclic group is isomorphic to $(Z,+)$

Proof. Let $G=\{x^0,x^1,x^2,\ldots,x^{n-1}\}$.

Mapping is given by $f(x^k) = k$.

$f(x^k\, x^m)=f(x^{k+m})=k+m=f(x^k)+f(x^m)$ (homomorphis

One-to-one: $f(x^k)=0 \Leftrightarrow k=0$ and $a^k=e$.

Permutation Groups

If the set is given by $A = \{1, 2, 3, \ldots, n\}$ then let S_n denote the set of all permutations on A.

It forms a group under function composition.

An element of S_n is represented by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

We call S_n the symmetric group of degree n and call any subgroup of S_n a permutation group.

Permutation Groups

Cayley's Theorem. Every group is isomorphic to a permutation group.

Sketch of proof. Let G be a group with operation $*$. For each $x \in G$, we define $\lambda_x: G \longrightarrow G$ given by $\lambda_x(g) = x * g$ for all $g \in G$.

This function λ_x is a permutation on G.

Next we create a permutation group out of λ_x.

Now we define $f: G \longrightarrow S_n$ by $f(x)= \lambda_x$

Cayley's Theorem. Every group is isomorphic to a permutation group.

We define $f: G \longrightarrow S_n$ by $f(x)= \lambda_x$

One-to-one. Suppose f(a)=f(b). It follows $\lambda_a= \lambda_b$ and in particular $\lambda_a(e)= \lambda_b(e)$. Thus, a e = b e and then a = b.

Onto. It follows from definition of λ_x

Homomorphism. $f(a\, b) = \lambda_{ab}$, $f(a) \blacklozenge f(b)= \lambda_a \blacklozenge \lambda_a$

To prove $\lambda_{ab}= \lambda_a \blacklozenge \lambda_a$, we write $\lambda_{ab}(x)=(ab)x=a\,(bx)=\lambda_a(bx)=\lambda_a(\lambda_b(x))=(\lambda_a \blacklozenge \lambda_b)(x)$

Study Bee

- Lagrange's Theorem
- Cosets
- Cyclic Group
- Permutation Group
- Cayley's Theorem